لحظات حرجة
تحدد مستقبل الأمن الإلكترونى..

# الذكاء الاصطناعى يهاجم الذكاء الاصطناعى!

**فى** العام الماضى، نشــرت مؤسسة "جارتنر للأبحاث" تقريرا توقعــت فيه أنه بحلــول عام 2020 ســيتم تضمين وإدماج تقنية "الذكاء الاصطناعى" Artificial Inteligence-AI فى جميع المنتجــات والبرامج الجديدة. ومع نمــو قدرات الذكاء الاصطناعى بوتيرة ســريعة، يتوقع خبراء أمــن المعلومات أن تصبح تقنية الذكاء الاصطناعى بالغة الأهمية ليس فقط للحماية من الهجمات الإلكترونية، ولكن أيضا لشــن الهجمات، وأن قدرة هذه التقنية على اتخاذ قرارات آلية للقيــام بهجمات إلكترونية ســتؤدى إلى إحداث ثورة فى مشــهد الأمن الإلكترونى كما نعرفه اليوم، من منظور دفاعى وهجومي.

كما هو الحال مع العديد من التقنيات التى تعتبر سيفا ذا حدين، سيكون من المهم للمسئولين عن الأمن الإلكترونى فى المؤسسات والشركات، أن يكونوا على علم بجانبى الصورة للحيلولة دون الوقوع فريســة للهجمات التى يقودها الذكاء الاصطناعى ضدهم.

أشرف شهاب

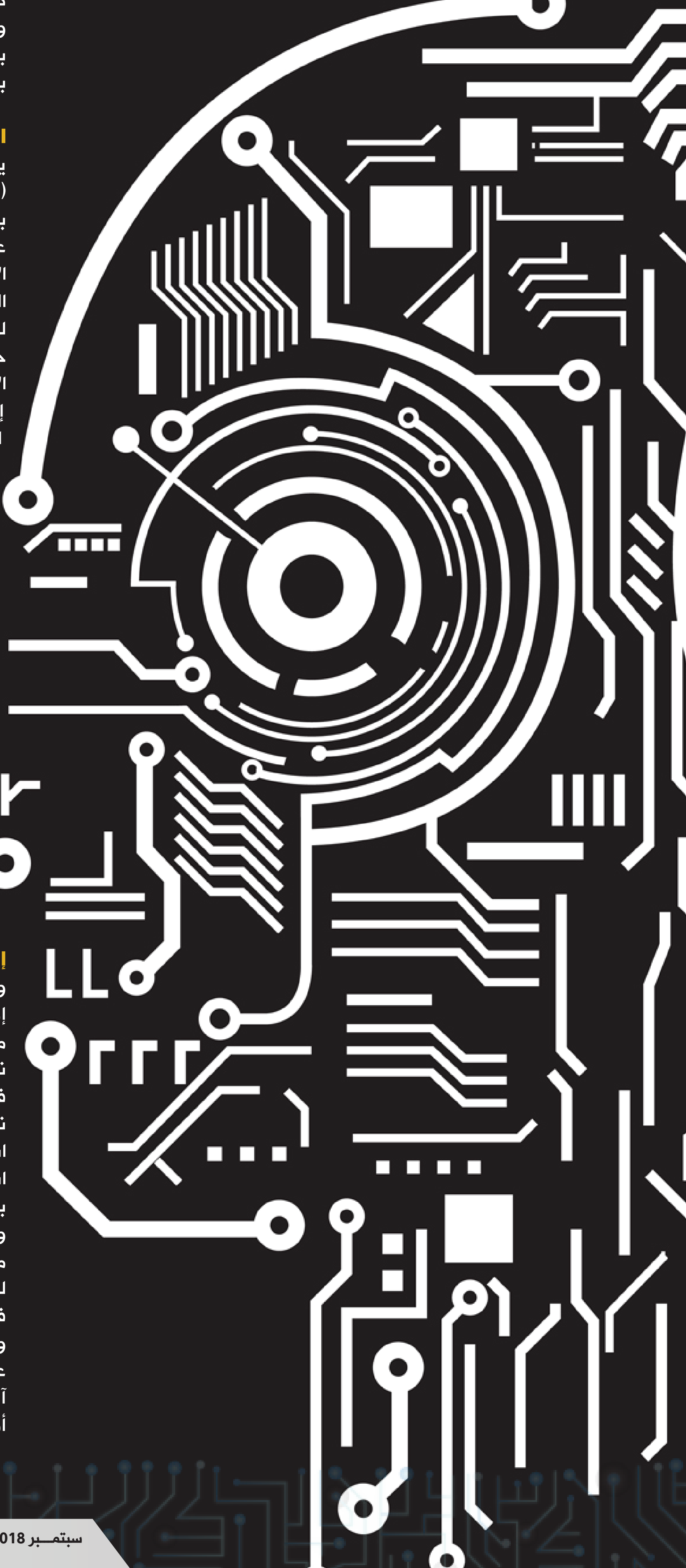
يهدف الذكاء الاصطناعى إلى أتمتة مجموعة واسعة من المهام. تتنوع ما بين الألعاب، والمركبات ذاتية القيادة، إلى الطائرات الموجهة بدون طيار (الدرونز)، والروبوتات، والأجهزة المنزلية، والآلات.
وباختصار، يمكن القول أن الذكاء الاصطناعى سيكون قادرا على القيام بمجموعة واسعة من المهام ، أو يمكن أن تكون أى مهمة قد يقوم بها البشر أو الحيوانات هدفا للابتكار من جانب علماء الذكاء الاصطناعى.

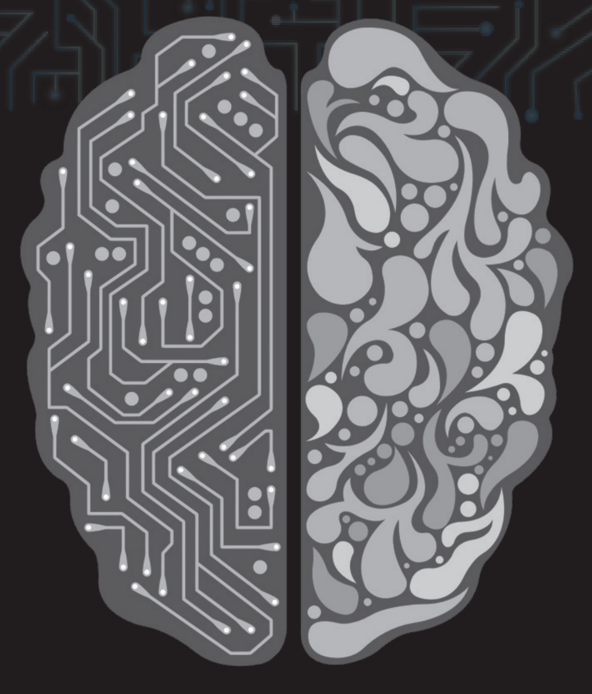
## التعلم الآلى والذكاء الاصطناعى

يتضمن الذكاء الاصطناعى، ضمن أقسامه ما يسمى: "التعلم الآلى" (Machine Learining)، وهو تمكين الآلات من التعلم، والقيام بالمهام بناء على قرارات تتخذها الآلات بأنفسها نتيجة خبراتها الذاتية، وقدراتها على تحليل السلوك البشرى، وتقليده. وفى مجال الأمن الإلكترونى يتم الاستفادة من قدرات الذكاء الاصطناعى على التعلم الآلى، بهدف تخفيف العبء عن العنصر البشرى لتأمين المعلومات والشبكات، فالتعلم الآلى لديه القدرة على مراقبة حركة المرور على الشبكة، ويمكنه بالتالى إنشاء خط الدفاع الأساسى للنظام ضد أى هجمات محتملة. كما يمكن للتعلم الآلى استخدام هذه المعلومات للإبلاغ عن أى نشاط مشبوه، بالاستناد إلى كميات هائلة من البيانات الأمنية التى يتم جمعها بواسطة خبراء الأمن الإلكترونى، الذين يقومون بدورهم بتعريف تلك المخاطر، ومن ثم تغذية الآلات بها مرة أخرى، لتمكينها من اتخاذ القرارات النهائية بشأن كيفية التصرف مستقبلا.
كما أن التعلم الآلى قادر أيضا على تصنيف النشاط الضار على مستويات مختلفة. على سبيل المثال، بالنسبة لطبقة الشبكة يمكن تطبيق التعلم الآلى للتعرف على هجمات "التطفل على النظام" Intrusion Network System (IDS) والهجمات الخداعية، وهجمات "رفض الخدمة" Denial of Service (DoS) وهجمات تعديل البيانات. كما يمكن تطبيقه طبقة تطبيقات الويب Web Application Layer (WAF) وطبقة نقطة النهاية Endpoint Layer لتحديد البرامج الضارة، وبرامج التجسس، وفيروسات الفدية Ran-someare.
ومن نافلة القول، أن التعلم الآلي، إن لم يكن بالفعل، عنصرا أساسيا فى مجموعة الأدوات التى يجب أن يستخدمها مسئولو الأمن الإلكترونى خلال السنوات القليلة المقبلة، لا سيما وأن الهجمات الإلكترونية أصبحت أكثر تكرارا واستهدافا.

## إطفاء النار بالنار

ومع ذلك، فإن تنفيذ تقنيات الذكاء الاصطناعى للدفاع الإلكترونى يشبه إطفاء النار بالنار، حيث إن المتسللين والمجرمين الإلكترونيين أصبحوا مسلحين بنفس نوعية الذخيرة، ويمتلكون نفس القدرات، مما يجعلنا نبدو وكأننا فى سباق تسلح لا نهاية له.
ففى بداية العام الحالى، حذر تقرير حول استخدام الذكاء الاصطناعى، نشرته أيضا، مؤسسة "جارتنر" للأبحاث، من أن الذكاء الاصطناعى يمكن استغلاله من قبل المتسللين لأغراض خبيثة، الذين يمتلكون القدرة على استهداف أنظمة كمبيوتر، وشبكات، بل، ودول بأكملها، مما يجعل العالم بأكمله يعيش "لحظات حرجة" فى التطور المشترك للذكاء الاصطناعى والأمن الإلكترونى، يستوجب أن نستعد بشكل استباقى للموجة القادمة من الهجمات.
لذا، ليس من المستغرب أن يهتم خبراء الأمن الإلكترونى بهذه القضية، فالذكاء الاصطناعى الذى يتم النظر إليه كأداة مثالية لحماية الشبكات والمعلومات، وتحليل بيانات الدفاع ضد الهجمات، ومراقبة حركة مرور على الشبكة، يمكن استخدامه أيضا من جانب المجرمين لاتخاذ قرارات آلية حول: من؟ وماذا؟ ومتى يجب البدء فى الهجوم؟!. ومن المتوقع بقوة أن يقوم الهاكرز باستخدام الذكاء الاصطناعى لسرقة بيانات المؤسسات





أو تغييرها أو تخريبها تماما، مما يتسبب فى أضرار جسيمة لسمعة الشركات وأرباحها، وأسعار أسهمها.

## الأكثر فعالية

لقد أصبح بإمكان المجرمين الإلكترونيين بالفعل استخدام الذكاء الاصطناعى للقيام بهجماتهم ضد الأفراد والمؤسسات عن طريق جمع المعلومات حول الأهداف من وسائل الإعلام الاجتماعية وغيرها من المصادر المتاحة للجمهور. وكمثال على ذلك: قامت شركة Zero-FOX المتخصصة فى الأمن الإلكترونى، مؤخرا بتجربة لتحديد الوسيلة الأكثر فاعلية فى جعل مستخدمى موقع التواصل الاجتماعى "تويتر" ينقرون على الروابط الضارة: البشر أم الذكاء الاصطناعى. أرسل الذكاء الاصطناعي، وتم خلال التجربة استخدام حساب يسمى:SNAP_R لإرسال "رسائل" "تغريدات" تصيد احتيالى إلى أكثر من 800 مستخدم بمعدل 6.75 تغريدة فى الدقيقة. ونتيجة للتجربة، تم خداع حوالى 275 شخصا. واتضح فى النهاية أن الذكاء الاصطناعى كان الأكثر فعالية فى العمل.

## الوقاية من الذكاء الاصطناعى

يعتقد الخبراء أن هناك 3 خطوات رئيسية ينبغى على خبراء الأمن الإلكترونى وضعها بعين الاعتبار لتعزيز دفاعاتهم ضد الهجمات التى يتم شنها باستخدام تقنيات الذكاء الاصطناعى:

### ـ تحديد ما يجب حمايته

بمجرد أن يفهم خبير الأمن الإلكترونى ما الذى يجب عليه حمايته بوضوح، يمكنه تنفيذ خطط دفاعية ووضع الحلول المناسبة لإدارة الحماية بشكل صحيح، والتعرف على نقاط الضعف ونقاط التهديد. وبالتالى ضمان تشفير البيانات الهامة، ووضع تصور كامل للخطط الدفاعية. ومن الضرورى أن تتضمن تلك الخطط الدفاعية وضع بدائل وخيارات لتغيير الاستراتيجية الدفاعية بسرعة وقت اللزوم، حيث أن المهاجمين دائما ما يتحركون بشكل سريع ومتغير.

### ـ وضع تصورات مستقبلية

يمكن للمنظمات امتلاك أفضل تكنولوجيا دفاعية فى العالم، ولكنها فعالة فقط للقيام بالعمليات المطلوبة منها. تتمثل المشكلة هنا فى أن الهجمات ستكون ذكية، وستحاول الالتفاف والتفوق على النظام، وبالتالى يجب التخطيط على نطاق أوسع للإجراءات المطلوبة، مع تثقيف الموظفين وتدريبهم على أفضل الممارسات الأمنية الإلكترونية.

### ـ تحديد ما هو مناسب لطبيعة العمل

يجب أن يتوافر فهم واضح لبيئة ودورة العمل، لتحديد ما هو مناسب للحماية. وغالبا ما تفشل الشركات فى هذه النقطة. إن امتلاك فهم واضح للموجودات وكيفية ترابطها فى بيئة العمل، يسمح للمؤسسات بعزل الأحداث غير الطبيعية، المشكوك فيها بشكل صحيح، والتحقيق فيها. ومن المفارقات، أن التعلم الآلى يعتبر أداة فعالة للغاية لتوفير هذا السياق، ولكن القدرات التكنولوجية، والأساليب التكتيكية التى يستخدمها المجرمون الإلكترونيون تتطور أيضا.

## خدعة الذكاء الاصطناعى

صاحبت عملية نشر تقنيات "الذكاء الاصطناعى" الكثير من المبالغات، والتهويلات فى قدراته، مما خلق حالة من الارتباك والغموض. ودفعت هذه الضجة والاهتمام المتزايد بالذكاء الاصطناعى بائعى البرامج إلى إدخال الذكاء الاصطناعى فى استراتيجية منتجاتهم. وطبقا لتقرير نشرته "جارتنر للأبحاث" لم يكن مصطلح "الذكاء الاصطناعي" ضمن أكثر 100 عبارة يتم البحث عنها على موقع الشركة Gartner.com فى شهر يناير 2016 ولكن بحلول شهر مايو 2017 احتل المصطلح الرقم 7 فى أكثر المصطلحات بحثا على الموقع، مما يشير إلى شعبية الموضوع، والاهتمام الذى أبداه العملاء لفهم كيفية استخدام الذكاء الاصطناعى كجزء من استراتيجية الأعمال الرقمية الخاصة بهم. وطبقا لذلك، يعتبر الذكاء الاصطناعى فرصة ذهبية للشركات، ولكن، لسوء الحظ، يركز معظم البائعين لتقنيات الذكاء الاصطناعى على تسويق منتجاتهم بدلا من التركيز على احتياجات العملاء، والاستخدامات المحتملة، والقيمة التجارية التى ستعود عليهم. فالحلول التى يقدمها الذكاء الاصطناعى متنوعة، ويجب أن يتم التركيز على تسويق ما يحتاجه العميل بدقة.

## سيناريوهات التهديد

بما أن قدرات الذكاء الاصطناعى أصبحت أكثر قوة وانتشارا، فمن المتوقع أن يؤدى الاستخدام المتزايد لها إلى تغييرات واسعة النطاق فى طبيعة ونوعية التهديدات على أمن المعلومات. ومن خلال خصائص الذكاء الاصطناعى التى أشرنا إليها، نستنتج ثلاثة سيناريوهات عالية المستوى للتهديدات التى يحملها الذكاء الاصطناعى فى غياب تطوير دفاعات كافية.

### أولا: توسيع التهديدات القائمة

من المتوقع أن يحرز الذكاء الاصطناعى تقدما فى مجال توسيع مجموعة الجهات القادرة على تنفيذ الهجمات، ومعدل الهجمات الذى يمكن لتلك الجهات القيام به، وكذلك مجموعة الأهداف المحتملة للهجوم. ويمكن أن يؤدى نشر أنظمة الذكاء الاصطناعى الفعالة إلى زيادة عدد العناصر القادرة على القيام بالهجمات. وإذا كانت أنظمة الذكاء الاصطناعى الدفاعية لا تتمتع بالكفاءة اللازمة، فعندئذ يمكن للمهاجمين المسلحين بالذكاء الاصطناعى القيام بالهجمات بمعدلات أعلى بكثير مما كان يحدث سابقا.

كما سيصبح من المجدى للمجرمين مهاجمة الأهداف التى لم يكن من المنطقى الهجوم عليها سابقا من وجهة نظر تحديد الأولويات أو تحليل التكلفة والعائد من الهجمات.

وعلى سبيل المثال، كانت هجمات التصيد الاحتيالي، تتطلب مجهودا لإرسال رسائل مخصصة لاستخراج المعلومات الحساسة أو إبتزاز الأفراد، حيث كان على المهاجم أن يقدم نفسه كأحد أصدقاء أو أقارب الضحية. وكان على المهاجم تحديد الأهداف ذات القيمة العالية، والقيام بمجهود بحثى فى الشبكات الاجتماعية والمهنية لتحديد هذه الأهداف، ثم توليد رسائل مناسبة لكل حالة على حدة. كما كانت الهجمات تتوقف مثلا إذا كان الضحية لا يتحدث بنفس لغة المهاجم. ولكن مع تقنيات الذكاء الاصطناعى سيكون من السهل تفادى كل تلك العقبات. كما أن قيام الآلات بتحمل العبء الأكبر فى الهجوم سيدفع المهاجمين لتوسيع هجماتهم لتشمل ضحايا أكثر، وتوسيع نطاق الإبتزاز المالى للقبول بمبالغ فدية أقل، والتنكر بسهولة، وتفادى عوائق اللغة وغيرها.

كما أن شعور المهاجمين بالأمان من خطر كشف هوياتهم سيشجع المزيد من المجرمين على القيام بهجماتهم. وفى حالة كان المهاجم لديه حد أدنى من الضمير ليتعاطف مع الضحية الضعيف، فإن هذا العائق أيضا سيزول، وسيتم الهجوم على الضحايا بدون أى تعاطف أو مشاعر إنسانية. وكذلك الأمر فى حالة كان المهاجم جبانا ويخشى ردة الفعل القوية من الضحية.

### ثانيا: ابتكار تهديدات جديدة

سيفتح التقدم فى الذكاء الاصطناعى المجال أمام أنواع جديدة من الهجمات لإنجاز مهام معينة بشكل أكثر نجاحا من أى إنسان، أو الاستفادة من نقاط الضعف التى تعانى منها أنظمة الذكاء الاصطناعى الدفاعية. فعلى سبيل المثال، لا يستطيع معظم الناس تقليد أصوات الآخرين بشكل واقعى لإنشاء ملفات صوتية تشبه صوت الضحية. ويساعد التقدم فى تطوير أنظمة محاكاة أصوات الأفراد (وهى تقنية يجرى تسويقها بالفعل)، وعدم القدرة على تمييزها عن الأصوات الأصلية على انتحال هوية الآخرين.

بالإضافة إلى ذلك، يمكن استخدام أنظمة الذكاء الاصطناعى للتحكم فى سلوك الروبوتات والبرامج الخبيثة التى يصعب على البشر التحكم فيها. كما أن نشر أنظمة جديدة من الذكاء الاصطناعى الدفاعية، يحمل مخاطر من تعرض تلك الأنظمة للهجمات التى تستغل أى ثغرات فيها. على سبيل المثال، يمكن أن يؤدى استخدام السيارات ذاتية القيادة إلى إعطاء فرصة للهجمات الإلكترونية التى تسبب الأعطال، أو الحوادث. ومن الممكن أن يتحكم نظام الذكاء الاصطناعى الهجومى فى عدة روبوتات فى نفس الوقت. وبالتالى فإن هجوما واحدا سيؤدى إلى سلسلة واسعة من الهجمات غير المتوقعة.

### ثالثا: تغيير الطابع التقليدى للتهديدات

سيتغير مشهد التهديدات من خلال توسيع التهديدات الحالية وظهور تهديدات جديدة لا وجود لها بعد، فالهجمات التى يدعمها ويمكنها التقدم بدعم من الذكاء الاصطناعى ستكون فعالة، وموجهة بدقة، ومن الصعب تحديدها. فبدلا من تفصيل الهجمات تبعا لكل حالة، سيمتلك المهاجمون الفرصة للقيام بهجمات جماعية، وبوتيرة أكبر. كما أن عدم الخوف من اكتشاف هوية المهاجم سيجعله أكثر عنفا، ورغبة فى القيام بالمزيد من الهجمات

## نماذج للمخاطر المتوقعة

يوفر استخدام تقنيات الذكاء الاصطناعى للمجرمين عدة فرص للقيام بهجمات والتسبب بأضرار لم تكن متوقعة مسبقا، عن طريق:

### أتمتة الهجمات

سيتمكن المهاجمون من استخدام معلومات الضحايا عبر الإنترنت لإنشاء مواقع إنترنت، أو بريد إلكترونى، أو إرسال روابط خبيثة مخصصة تلقائيا للضحايا من عناوين تنتحل شخصية جهات الاتصال الحقيقية الخاصة بهم، وذلك باستخدام أنماط كتابة تشبه الأنماط الحقيقية. ومع تطور الذكاء الاصطناعى، يمكن من خلال تلك المواقع إشراك الناس فى حوارات أطول، وربما التنكر بصريا كشخص آخر فى دردشة فيديو.

#### 1. اكتشاف الثغرات

يتم استغلال نقاط ضعف التعليمات البرمجية لتسريع اكتشاف ثغرات جديدة، واستغلالها فى الهجوم.

#### 2. قرصنة أكثر تعقيدا

يمكن استخدام الذكاء الاصطناعى، بشكل مستقل أو بالتنسيق مع البشر، لتحسين عملية تحديد الأهداف، وتحديد الأولويات، والتهرب من الكشف، والاستجابة الإبداعية التفاعلية للمتغيرات فى سلوك الضحايا.

#### 3. رفض الخدمة

تقليدا للسلوك الإنسانى، يمكن تقليد أنماط النقرات البشرية على الروابط (اللنكات)، وأنماط تصفح الإنترنت للهجوم على المواقع، وبالتالى إعاقة وصول المستخدمين إليها.

#### 4. أتمتة خطوات الجريمة

يستخدم مجرمو الإنترنت تقنيات الذكاء الاصطناعى لأتمتة المهام الهجومية المختلفة، مثل: معالجة عمليات الدفع المالى، أو الحوار مع ضحايا فيروسات الفدية.

#### 5. تحديد أولويات الأهداف

يمكن تحليل البيانات التى يتم جمعها لتحديد هوية الضحايا بشكل أكثر كفاءة، على سبيل المثال: تقدير الثروة الشخصية للفرد، وتقدير مدى استعداده للدفع على أساس سلوكياته السابقة عبر الإنترنت.

#### 6. تسميم البيانات

يمكن القيام بهجمات لتسميم البيانات لتشويهها، أو إنشاء ثغرات خلفية فى نماذج التعلم الآلى الخاصة بالجهة المستهدفة بالهجوم.

#### 7. التحكم فى نظام الضحايا

يمكن القيام بهجمات بهدف استخراج المعلومات من نظام الذكاء الاصطناعى للضحايا عن طريق إرسال مدخلات بشكل منتظم، ومراقبة نواتجها، وبالتالى استنتاج العيوب والثغرات التى تتيح للمهاجم التحكم فى نظام الذكاء الاصطناعى للضحية.

#### 8. القيام بعمليات إرهابية

يمكن للمجرمين استخدام الأنظمة التجارية بطرق ضارة، مثل التحكم فى الطائرات بدون طيار أو المركبات ذاتية القيادة لإيصال المتفجرات، أو التسبب فى الأعطال.

#### 9. اكتساب المهارات

يمكن للأتمتة التى يدعمها الذكاء الاصطناعى أن تمنح مهارات عالية للمجرمين ذوى المهارات المنخفضة، فعلى سبيل المثال يمكن التحكم الآلى فى الطائرات بدون طيار، أو السيارات ذاتية القيادة، فى حين أن المهاجم بمفرده لا يمكن له القيام بذلك.

#### 10. مسح آثار الهجمات

يمكن للمجرم إزالة آثار الهجوم، ووقته، ومكانه، من خلال سلسلة من عمليات التمويه المعقدة.

#### 11. تقارير وهمية وفيديوهات

يمكن تصنيع مقاطع فيديو واقعية للغاية لأى شخص، بما فى ذلك قادة ورؤساء الدول، وإظهارهم، وكأنهم يقدمون تعليقات تحريضية لم يقوموا بها فى الواقع.

#### 12. أتمتة حملات التضليل

يمكن استهداف الأفراد فى المناطق المضطربة برسائل مخصصة للتأثير على سلوكهم، مثلا فى الحملات الانتخابية.

#### 13. أتمتة حملات التأثير

تتم الاستفادة من التحليلات المدعومة بالذكاء الاصطناعى لشبكات التواصل الاجتماعى لتحديد الشخصيات المؤثرة الرئيسية، والتى يمكن عندئذ استهدافها بالمعلومات المضللة.

#### 14. هجمات التشويش المعلوماتى

يتم الاستفادة من هجمات توليد المعلومات على نطاق واسع وبوتيرة عالية لإغراق قنوات المعلومات بالكاذبة، مما يجعل من الصعب الحصول على المعلومات الحقيقية.

#### 15. التوجيه

يتم استخدام خوارزميات معينة لتوجيه المستخدمين نحو محتوى معين أو إبعادهم عن محتوى آخر.